MINISTER FOR CORRECTIVE SERVICES — PORTFOLIOS — CYBERSECURITY BREACHES

6317. Mr S.K. L'Estrange to the Minister for Emergency Services; Corrective Services:

I refer to each Department, Agency and Government Trading Enterprise within the Minister's portfolio of Corrective Services, and I ask:

(a) Were there any cybersecurity breaches to agency computer systems or servers in 2017;

(b) If yes to (a), for each breach:

(i) When did the breach occur;

(ii) What entity was responsible for each breach and what was their suspected purpose;

(iii) What information was compromised; and

(iv) How did the breach occur and what action has been taken to stop a recurrence of this breach;

(c) Were there any cybersecurity breaches to agency computer systems or servers in 2018;

(d) If yes to (c), for each breach:

(i) When did the breach occur;

(ii) What entity was responsible for each breach and what was their suspected purpose;

(iii) What information was compromised; and

(iv) How did the breach occur and what action has been taken to stop a recurrence of this breach;

(e) Were there any cybersecurity breaches to agency computer systems or servers in 2019; and

(f) If yes to (e), for each breach:

(i) When did the breach occur;

(ii) What entity was responsible for each breach and what was their suspected purpose;

(iii) What information was compromised; and

(iv) How did the breach occur and what action has been taken to stop a recurrence of this breach?

Mr F.M. Logan replied:

(a) Yes.

(b) (i) 11th January 2017.

(ii) Unknown.

(iii) Unknown.

(iv) A user clicked on a link from a news website and was further instructed to contact a technician for IT support which they did. The call was disconnected before the end of their conversation. The user immediately alerted the IT Department of the incident. IT reset the users passwords, wiped and rebuilt the PC. To minimise the chances of recurrence, the Department of Justice conducted social engineering awareness raising exercises and undertook an internal social engineering audit.

(c) No.

(d) Not applicable.

(e) Yes.

(f) (i) 15th November 2019.

(ii) It was a phishing email. Unknown.

(iii) No.

(iv) The bank details of an employee were changed after Payroll received an email from an individual purporting to be a genuine employee of the Department. Once HR were alerted of the change, they immediately identified a security breach and the matter was reported to the fraud department of the employee's bank and to the WA Police. To minimise the chances of recurrence, the Department of Justice:

Immediately sent out a Cyber Security Advisory notification by email to all users alerting them of potential for social engineering attacks and reminding them to be vigilant against social engineering attempts.

Implemented changes in how payroll requests sent through email are assessed to ensure fraudulent requests are detected and reported. This includes directing employees to use the Department's HR Kiosk facility to make changes themselves, and where HR is required to make the change, they should phone the employee using a known employee’s phone number to confirm the change request, and when the change is made. HR then send an email to the employee using a known employee’s email address to confirm the change.

Implemented a mandatory online security awareness training program for all users in December 2019 to periodically remind users of their information security responsibilities, including identification, prevention and reporting of social engineering attacks.

Drafted an ICT Acceptable Use Policy that will be published in the third quarter of 2020 to clarify information security responsibilities for users, including responsibility for identifying and reporting potential and actual cyber security incidents.

Conducted an internal social engineering audit and raised awareness of social engineering risks and how users can prevent social engineering attacks from succeeding.